UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,384	03/02/2000	Simon Robert Walmsley	AUTH07US	4249

7590 12/02/2004

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/517,384	WALMSLEY, SIMON ROBERT	
	Examiner	Art Unit	
	Nga B. Nguyen	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 13, 2004 has been entered.

2. Claims 1-16 are pending in this application.

Response to Arguments/Amendment

3. Applicant's arguments with respect to claims 1-16 have been fully considered but are moot in view of new grounds of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 3-5, 7-11, and 13-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Shigenaga, U.S. Patent No. 4,710,613.

Regarding to claim 1, Shigenaga discloses a validation protocol for determining whether an untrusted authentication chip (column 6, lines 1-53, IC card 2 is equivalent to the untrusted authentication chip) is valid, or not, including the steps of:

generating an original random number (column 7, lines 45-48; a random number is generated from random number data generator 120 of card terminal 1);

applying, in the trusted authentication chip, an asymmetric encryption encrypted random number (column 7, lines 59-60, the RSA encrypter 121 in the card terminal 1 encrypts the random number using public key code, the card terminal 1 is equivalent to the trusted authentication chip, RSA encryption is asymmetric encryption function);

passing the encrypted random number to an untrusted authentication chip (column 7, lines 60-67, the encryption data, i.e. the encrypted random number is sent to IC card 2 from card terminal 1) ;

decrypting, in the untrusted authentication chip, the encrypted random number with an asymmetric decryption function using a second secret key from the untrusted authentication chip to produce a decrypted random number (column 7, line 65-column 8, line 12; decrypting in the IC card 2 the encrypted random number by the RSA decrypter 263 using the private key code from the IC card 2);

comparing the decrypted random number with the original random number, without knowledge of the second secret key, and in the event of a match considering the untrusted chip to be valid (column 8, lines 28-32, 63-66, the decrypted random number is compared with the original random number by the comparison unit 15, without knowledge of the private key code stored in the IC card 2);

otherwise considering the untrusted chip to be invalid (column 8, lines 32-42).

Regarding to claim 3, Shigenaga discloses the first key is a public key (column 7, lines 50-60).

Regarding to claim 4, Shigenaga discloses the encryption is implemented in software (column 8, lines 59-62; the encryption is implemented based on the RSA algorithm).

Regarding to claim 5, Shigenaga discloses the encryption is implemented in a second authentication chip (column 5, lines 20-67; the encryption is implemented in the card terminal 1).

Regarding to claim 7, Shigenaga discloses the system comprises:

a random number generator to generate an original random number (figure 2 and column 5, lines 20-31, random number generator 120);

an asymmetric encryptor to encrypt the original random numbers using a first key in a trusted authentication chip (figure 2 and column 5, lines 38-67; the RSA encrypter 121 in the card terminal 1);

an untrusted authentication chip to receives the encrypted random number, the untrusted chip including includes an asymmetric decryption function to decrypt the encrypted random number using a second secret key for the decryption function to produce a decrypted random number (column 6, lines 1-55; column 7, line 65-column 8, line 12; the IC card receives the encrypted random number from the card terminal 1, the IC card 2 includes the RSA decrypter 263 to decrypts the encrypted random number using a private key code to produce a decrypted random number);

a comparison means to compare the decrypted random number with the original random number, without knowledge of the second secret key (figure 2, column 2, lines 62-67 and column 8, lines 28-32, 63-66, the comparison unit 15 compares the decrypted random number with the original random number, without knowledge of the private key code stored in the IC card 2).

Whereby in the event of a match between the decrypted random number and the original random number, the untrusted chip is considered to be valid; otherwise is considered to be valid (column 8, lines 32-42, 63-66).

Regarding to claims 8, 9, Shigenaga discloses the random number generator, encryptor and comparison means are in an external system, the external system is in a device in which are mounted, and the untrusted chip is in the consumable (column 5, line 20-column 6, lines 55, the random number generator, encryptor and comparison means are in the card terminal 1, the IC card 2 is the consumable).

Regarding to claim 10, Shigenaga discloses the random number generator and encryptor are in a second authentication chip, and the comparison means are in an external system which receives the random number and the encrypted version before passing only the encrypted version to the untrusted chip; the system also receives back the decrypted version from the untrusted chip and performs the comparison (column 8, lines 13-42).

Regarding to claim 11, Shigenaga discloses the system is in a device in which consumable are mounted, and the untrusted chip is in the consumable (column 5, line 20-column 6, lines 55, the card terminal 1 and the IC card 2 is the consumable).

Claims 13-15 contain similar limitations found in claims 3-5 discussed above, therefore are rejected by the same rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2, 6, 12, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shin et al (hereinafter Shin), U.S. Patent No. 5,987,134.

Regarding to claims 2, 12, Shigenaga does not disclose the random number is not secret, but where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed. However, it is well known in the art to generate the random number from a seed, and the next random number is produced from a new seed in order to improve the level of security. Therefore, it would have been obvious to modify Shigenaga's to include the feature above for the purpose of providing high security level because each next random number is generated from a new seed, thus the unauthorized person cannot easily to predict the random number.

Regarding to claims 6, 16, Shigenaga does not disclose the keys used for encryption and decryption are 2048 bits or larger. However, it is well known in the art to

implement the encryption or decryption keys using 2048 or larger bits. Therefore, it would have been obvious to modify Shigenaga's to include the feature above for the purpose of providing high security level because producing the encryption and decryption keys with larger bits makes the unauthorized person cannot easily to guess the keys.

Conclusion

8. Claims 1-16 are rejected.

9. The prior arts made of record and not relied upon is considered pertinent to applicant's disclosure:

Rikuma (US 4,827,113) discloses the technique for authenticating IC card and terminal.

Lee (US 5,923,759) discloses a system for securely exchanging data with smart cards.

Davis et al. (US 6,088,450) disclose the authentication system based on periodic challenge/response protocol.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (703) 306-2901. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (703) 308-0505.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 306-1113.

11. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

C/o Technology Center 3600

Washington, DC 20231

Or faxed to:

(703) 872-9326 (for formal communication intended for entry),

or

(703) 308-3691 (for informal or draft communication, please label "PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, Seventh Floor (Receptionist).

Nga B. Nguyen

Nga Nguyen

November 23, 2004